Access Control Lists

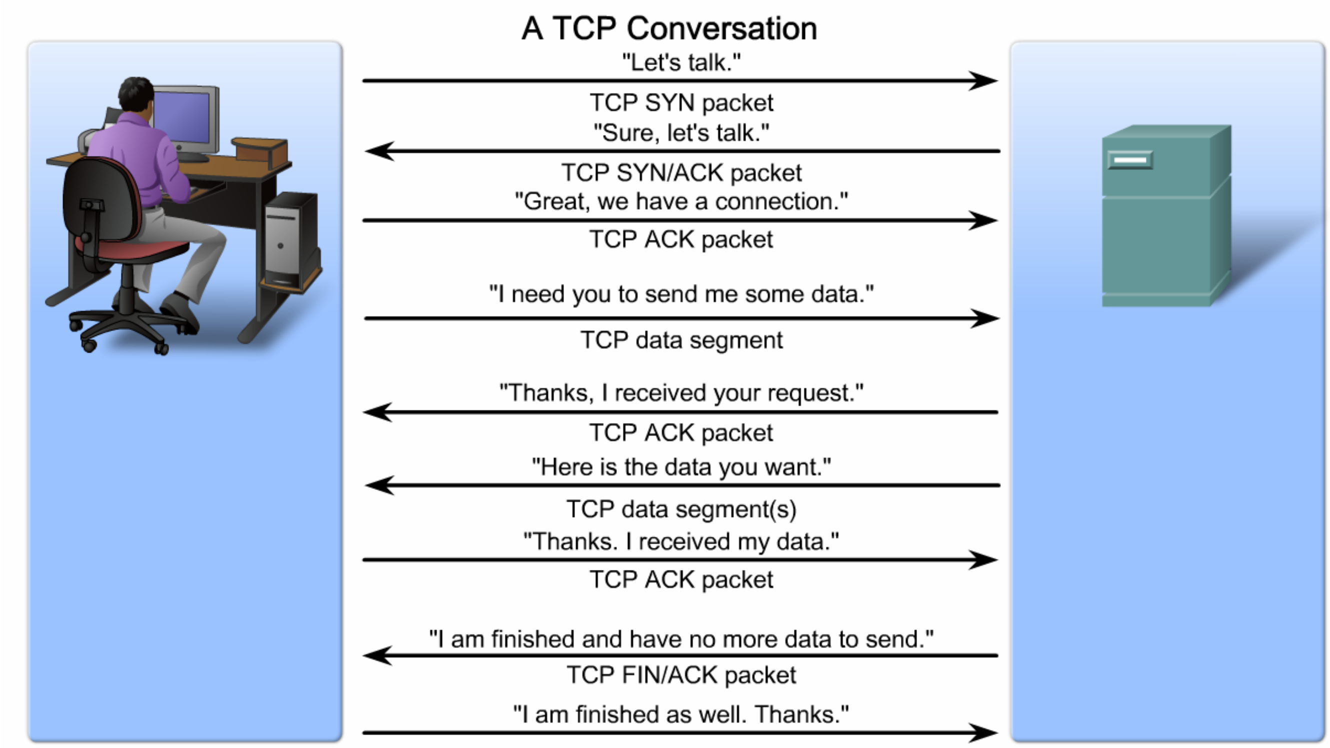
Accessing the WAN – Chapter 5

Objectives

- Explain how ACLs are used to secure a medium-size Enterprise branch office network.
- Configure standard ACLs in a medium-size Enterprise branch office network.
- Configure extended ACLs in a medium-size Enterprise branch office network.
- Describe complex ACLs in a medium-size Enterprise branch office network.
- Implement, verify and troubleshoot ACLs in an enterprise network environment.

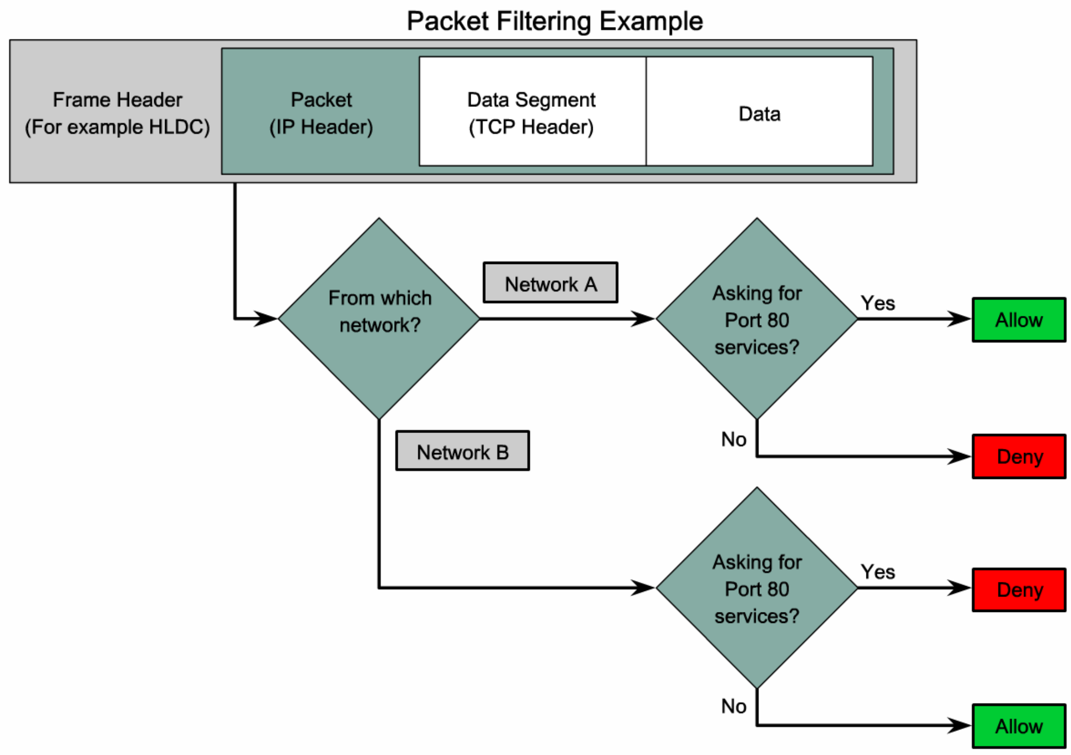
Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Describe the steps that occur in a complete TCP conversation


A TCP Conversation
"Let's talk."
TCP SYN packet
"Sure, let's talk."
TCP SYN/ACK packet
"Great, we have a connection."
TCP ACK packet
"I need you to send me some data."
TCP data segment
"Thanks, I received your request."
TCP ACK packet
"Here is the data you want."
TCP data segment(s)
"Thanks. I received my data."
TCP ACK packet
"I am finished and have no more data to send."
TCP FIN/ACK packet
"I am finished as well. Thanks."

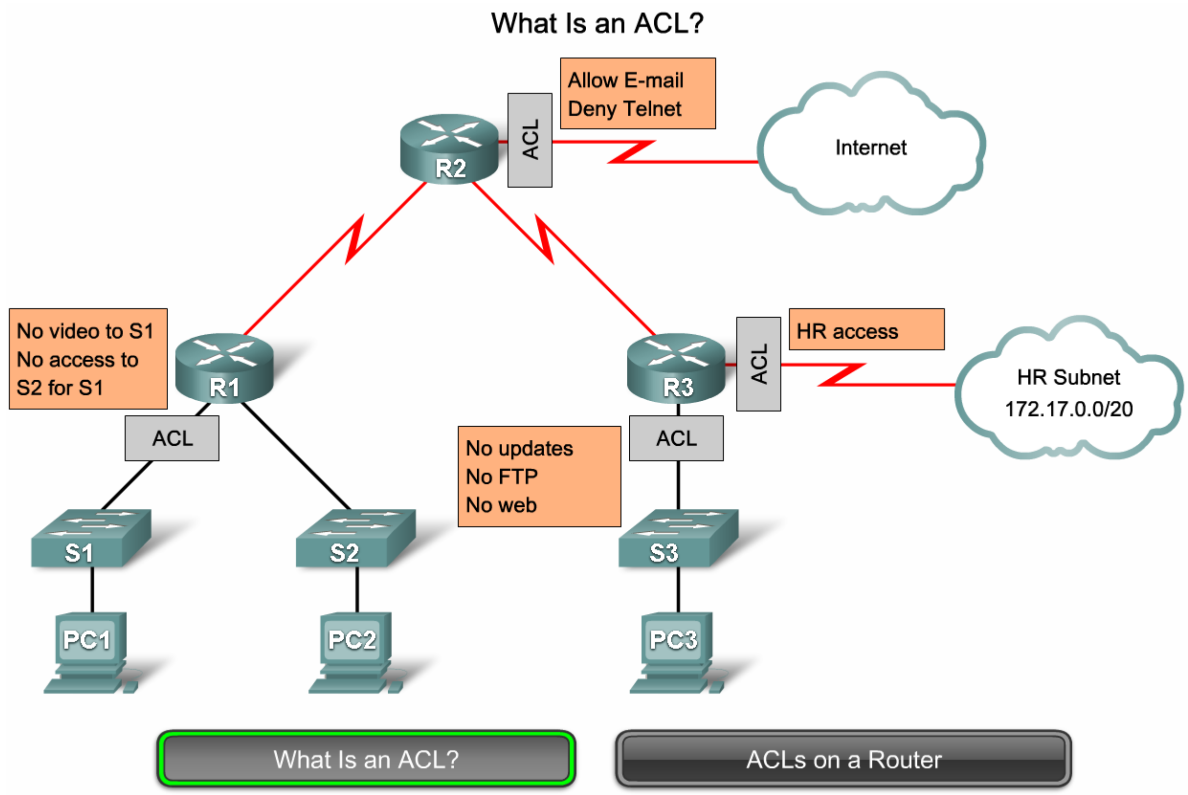
Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Explain how a packet filter allows or blocks traffic



Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Describe how ACLs control access to networks



What Is an ACL?

Allow E-mail
Deny Telnet

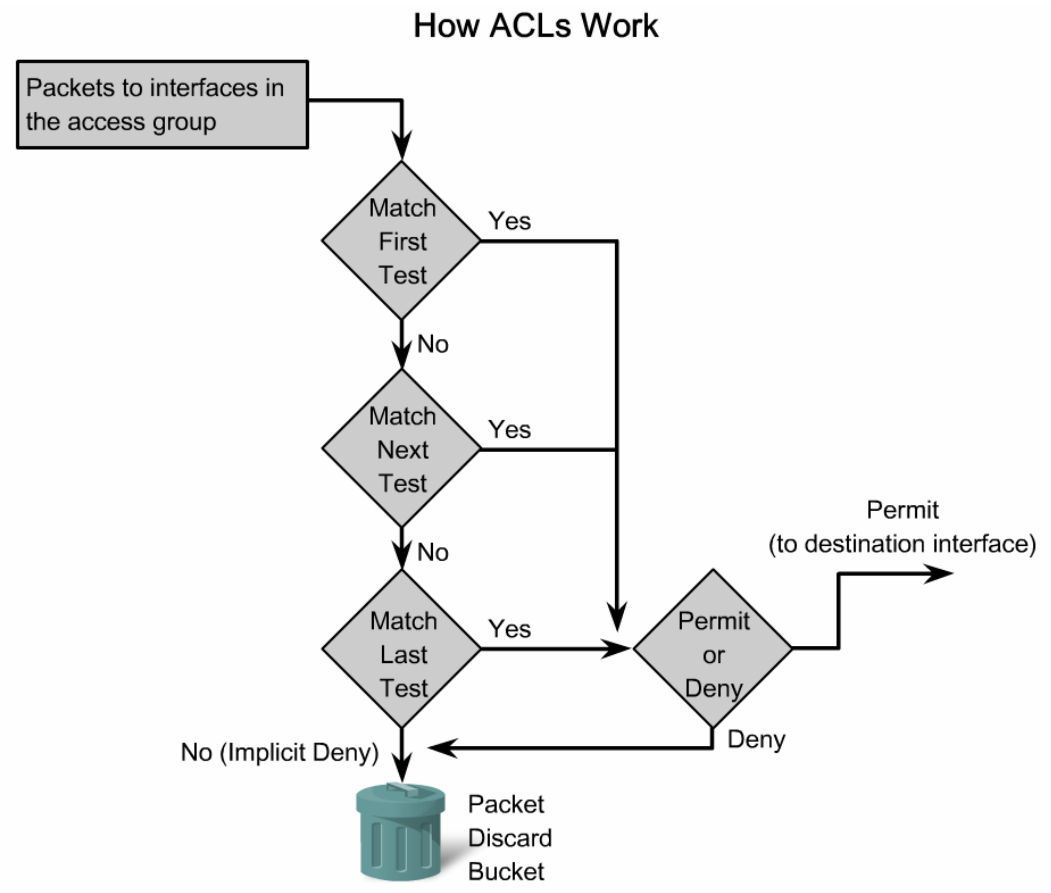
No video to S1
No access to S2 for S1

No updates
No FTP
No web

HR access

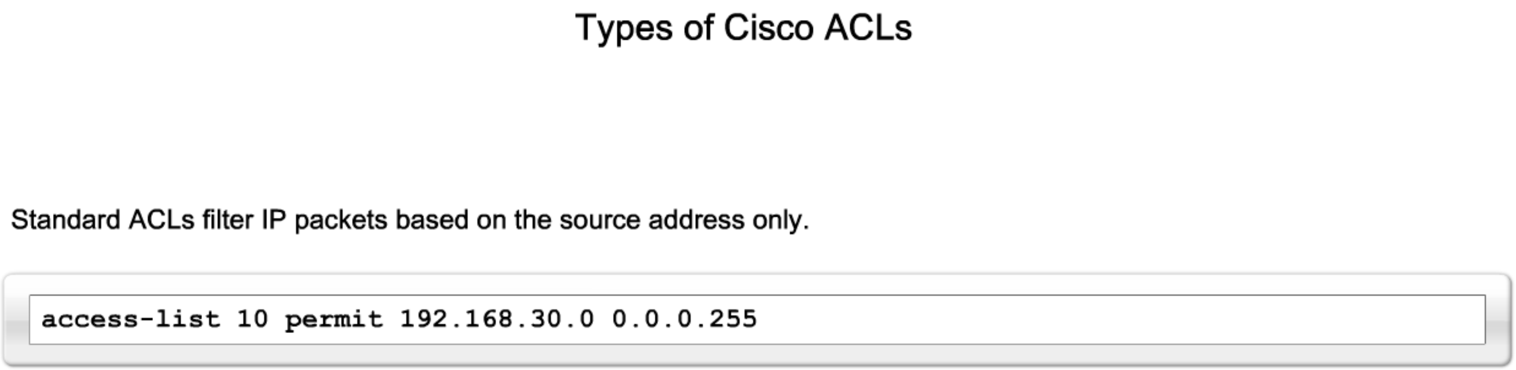
Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Use a flow chart to show how ACLs operate



Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Describe the types and formats of ACLs



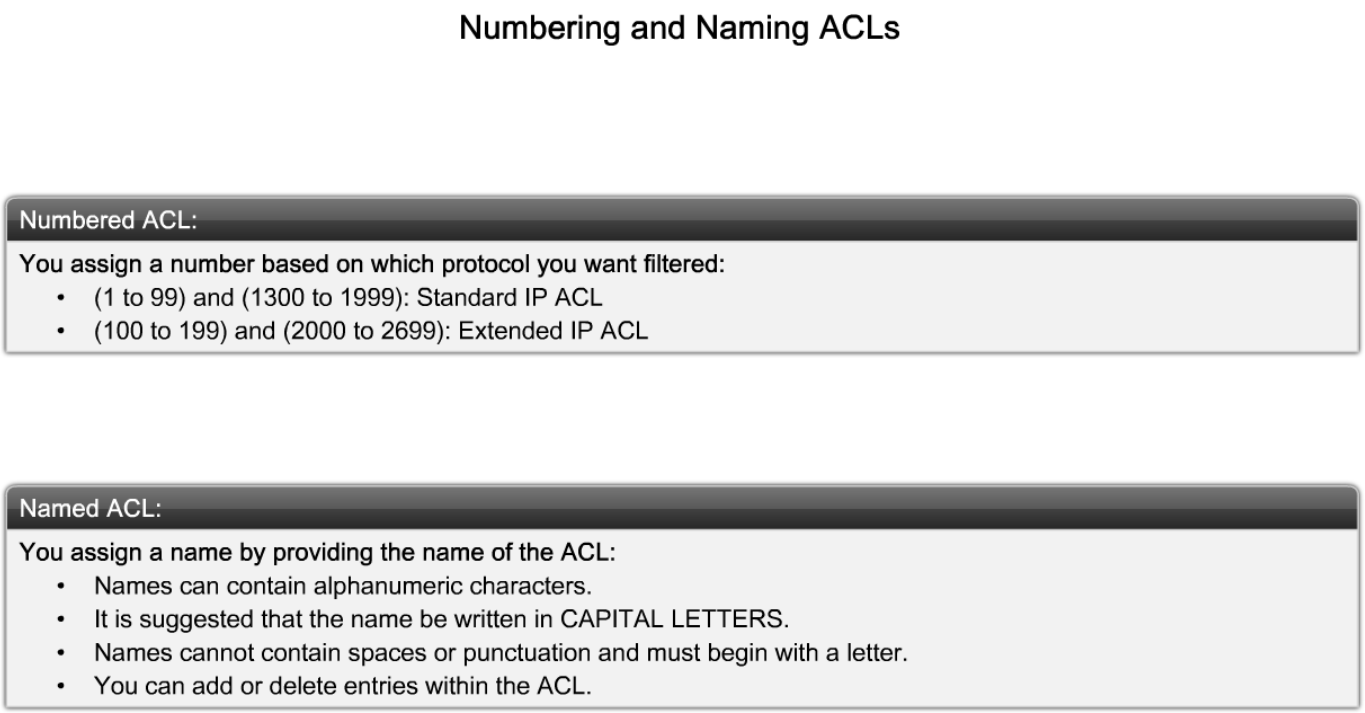
Types of Cisco ACLs

Standard ACLs filter IP packets based on the source address only.

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Explain how Cisco ACLs can be identified using standardized numbering or names



Numbering and Naming ACLs

Numbered ACL:

You assign a number based on which protocol you want filtered:

- (1 to 99) and (1300 to 1999): Standard IP ACL
- (100 to 199) and (2000 to 2699): Extended IP ACL

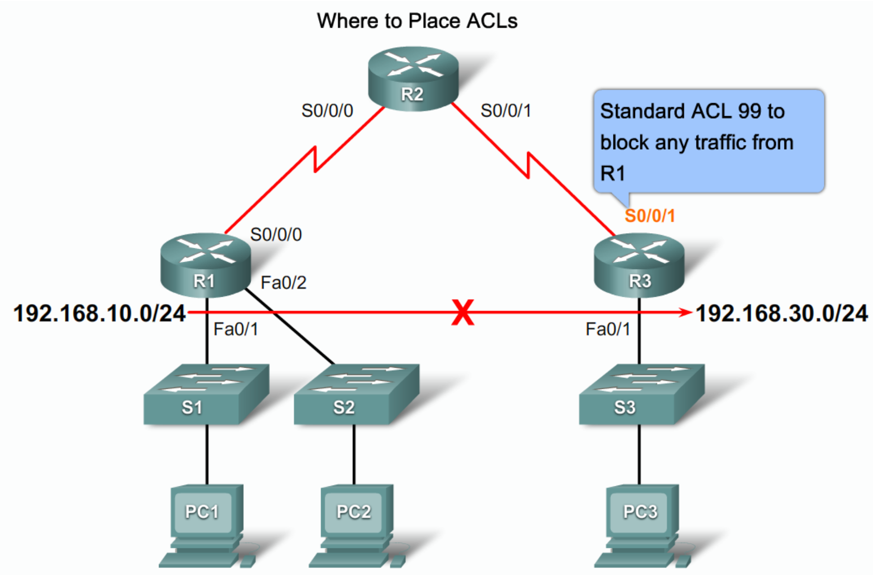
Named ACL:

You assign a name by providing the name of the ACL:

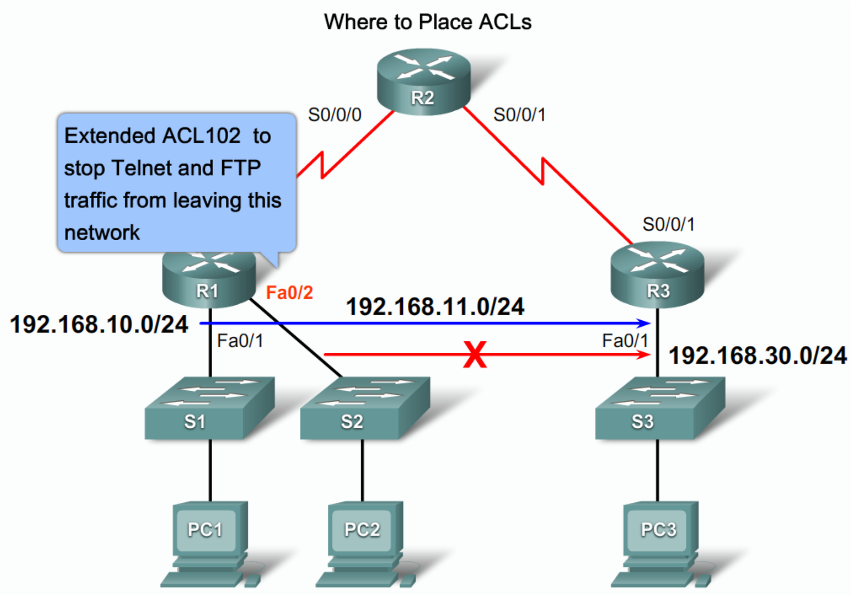
- Names can contain alphanumeric characters.
- It is suggested that the name be written in CAPITAL LETTERS.
- Names cannot contain spaces or punctuation and must begin with a letter.
- You can add or delete entries within the ACL.

Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Describe where ACLs should be placed in a network



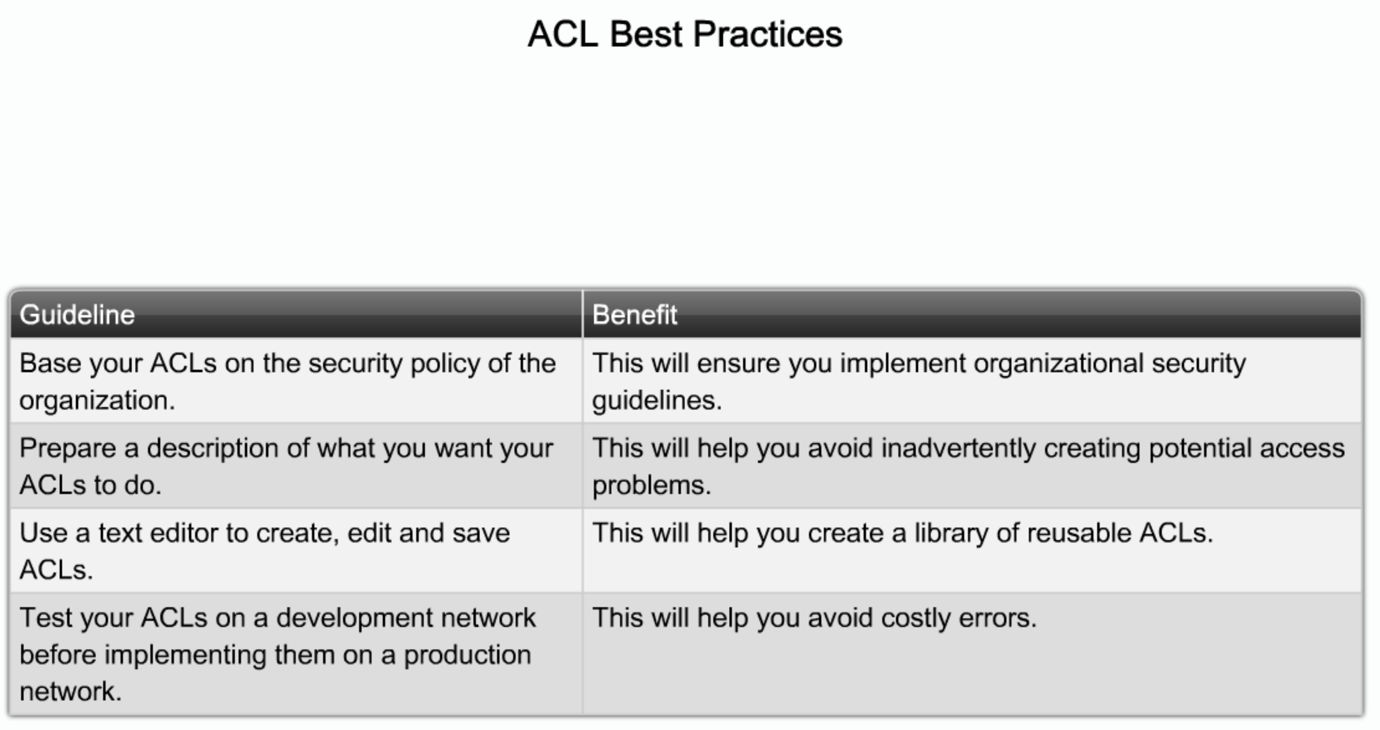
Standard ACL 99 to block any traffic from R1



Extended ACL102 to stop Telnet and FTP traffic from leaving this network

Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Explain the considerations for creating ACLs



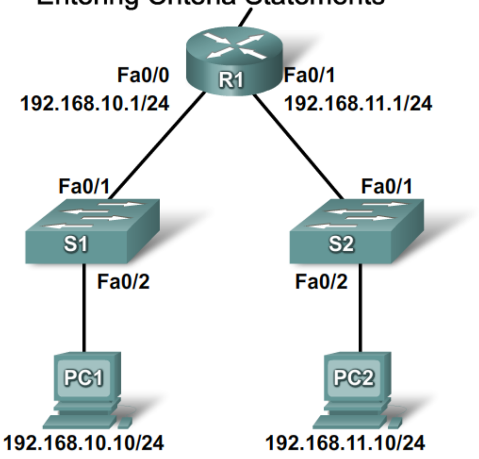
ACL Best Practices

Guideline	Benefit
Base your ACLs on the security policy of the organization.	This will ensure you implement organizational security guidelines.
Prepare a description of what you want your ACLs to do.	This will help you avoid inadvertently creating potential access problems.
Use a text editor to create, edit and save ACLs.	This will help you create a library of reusable ACLs.
Test your ACLs on a development network before implementing them on a production network.	This will help you avoid costly errors.

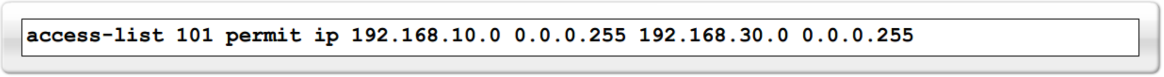
Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Explain why the order in which criteria statements are entered into an ACL is important

Entering Criteria Statements

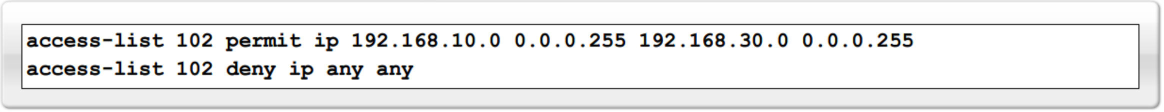


ACL 101



```
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

ACL 102

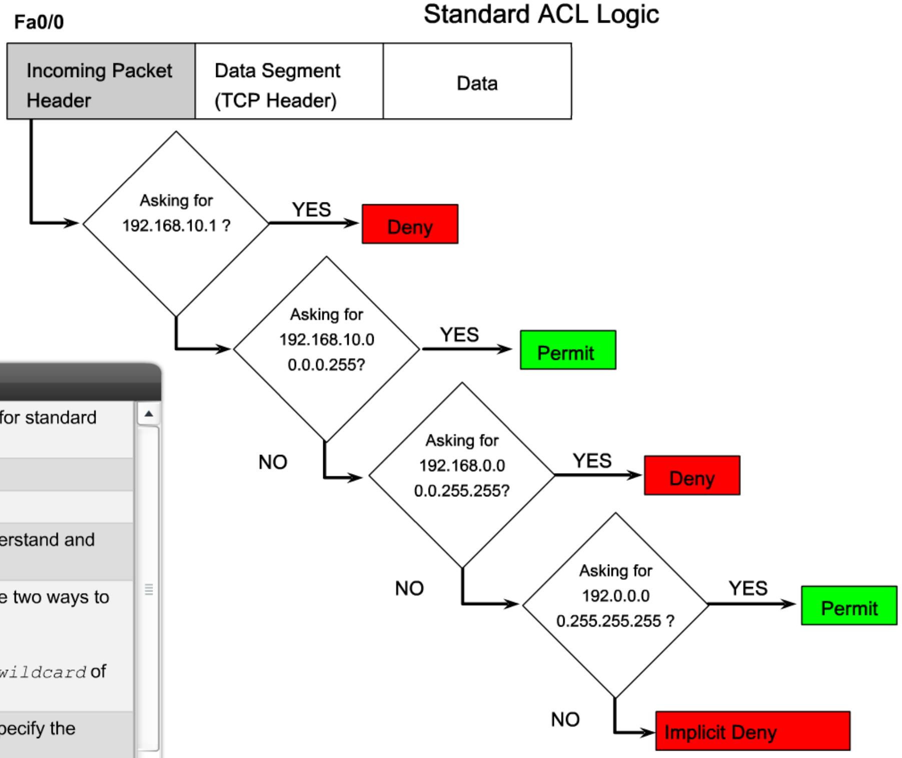


```
access-list 102 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 102 deny ip any any
```

Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Explain how to configure a standard ACL

Standard ACL Logic


Fa0/0
Incoming Packet Header
Data Segment (TCP Header)
Data
Asking for 192.168.10.1 ?
YES
Deny
Asking for 192.168.10.0 0.0.0.255?
YES
Permit
NO
Asking for 192.168.0.0 0.0.255.255?
YES
Deny
NO
Asking for 192.0.0.0 0.255.255.255 ?
YES
Permit
NO
Implicit Deny

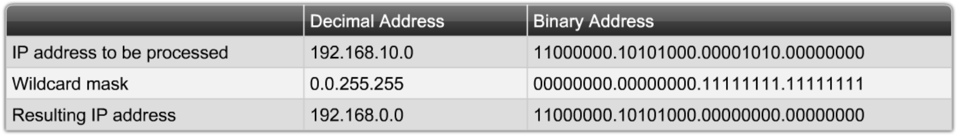
Standard ACL **access-list** Command Syntax

Parameter	Description
access-list-number	Number of an ACL. This is a decimal number from 1 to 99, or 1300 to 1999 (for standard ACL).
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
remark	Add a remark about entries in an IP access list to make the list easier to understand and scan.
source	Number of the network or host from which the packet is being sent. There are two ways to specify the *source*: • Use a 32-bit quantity in four-part, dotted- decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.55.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are two ways to specify the source-wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.55.
log	(Optional) Causes an informational logging message about the packet that matches the

Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Describe how to use wildcard masks with ACLs

Wildcard Mask Example



	Decimal Address	Binary Address
IP address to be processed	192.168.10.0	11000000.10101000.00001010.00000000
Wildcard mask	0.0.255.255	00000000.00000000.11111111.11111111
Resulting IP address	192.168.0.0	11000000.10101000.00000000.00000000

Wildcard Mask Calculation - 1

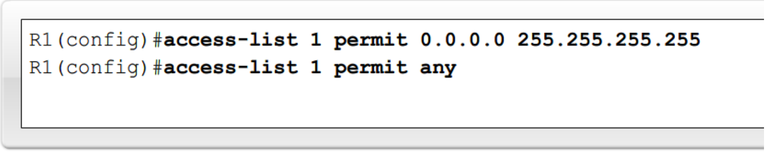
```
  255.255.255.255
- 255.255.255.000
  ---------------
  000.000.000.255
```

Wildcard Mask Calculation - 2

```
  255.255.255.255
- 255.255.255.240
  ---------------
  000.000.000.015
```

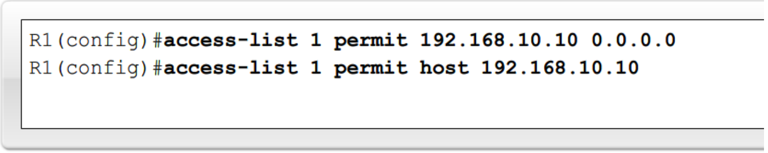
The **any** and **host** Keywords

Example 1:



```
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 permit any
```

Example 2:

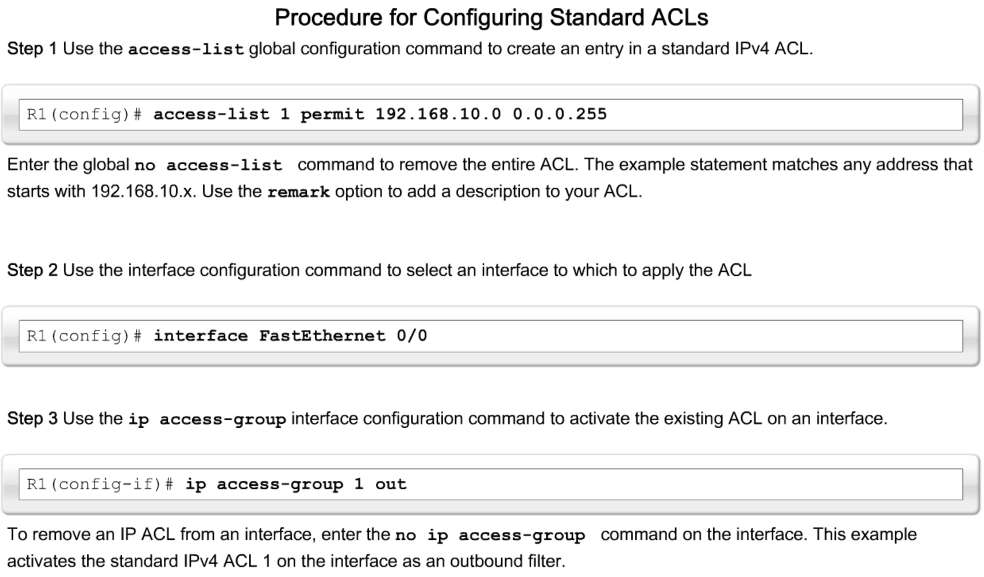


```
R1(config)#access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit host 192.168.10.10
```

This is the format of the host and any optional keywords in an ACL statement.

Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Describe how to apply a standard ACL to an interface



Procedure for Configuring Standard ACLs

Step 1 Use the **`access-list`** global configuration command to create an entry in a standard IPv4 ACL.

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

Enter the global **`no access-list`** command to remove the entire ACL. The example statement matches any address that starts with 192.168.10.x. Use the **`remark`** option to add a description to your ACL.

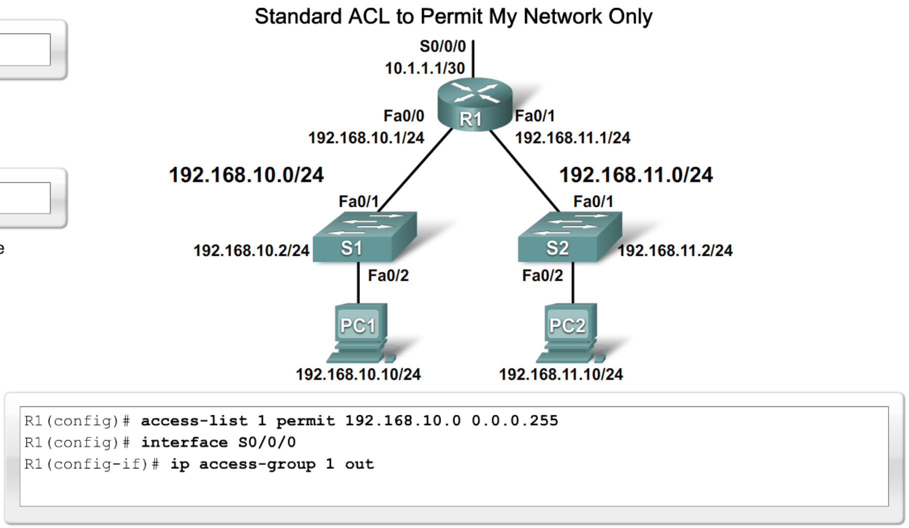
Step 2 Use the interface configuration command to select an interface to which to apply the ACL

```
R1(config)# interface FastEthernet 0/0
```

Step 3 Use the **`ip access-group`** interface configuration command to activate the existing ACL on an interface.

```
R1(config-if)# ip access-group 1 out
```

To remove an IP ACL from an interface, enter the **`no ip access-group`** command on the interface. This example activates the standard IPv4 ACL 1 on the interface as an outbound filter.



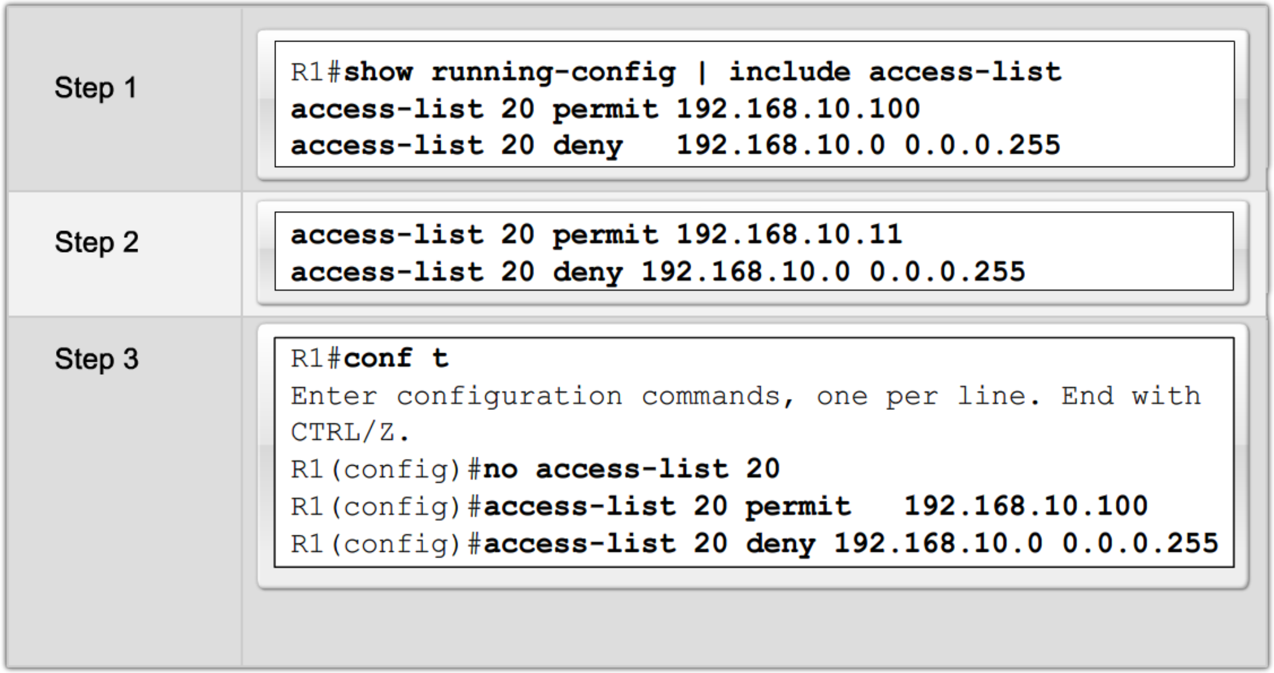
Standard ACL to Permit My Network Only

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 1 out
```

Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Explain the process for editing numbered ACLs

Editing Numbered ACLs



Step 1

```
R1#show running-config | include access-list
access-list 20 permit 192.168.10.100
access-list 20 deny   192.168.10.0 0.0.0.255
```

Step 2

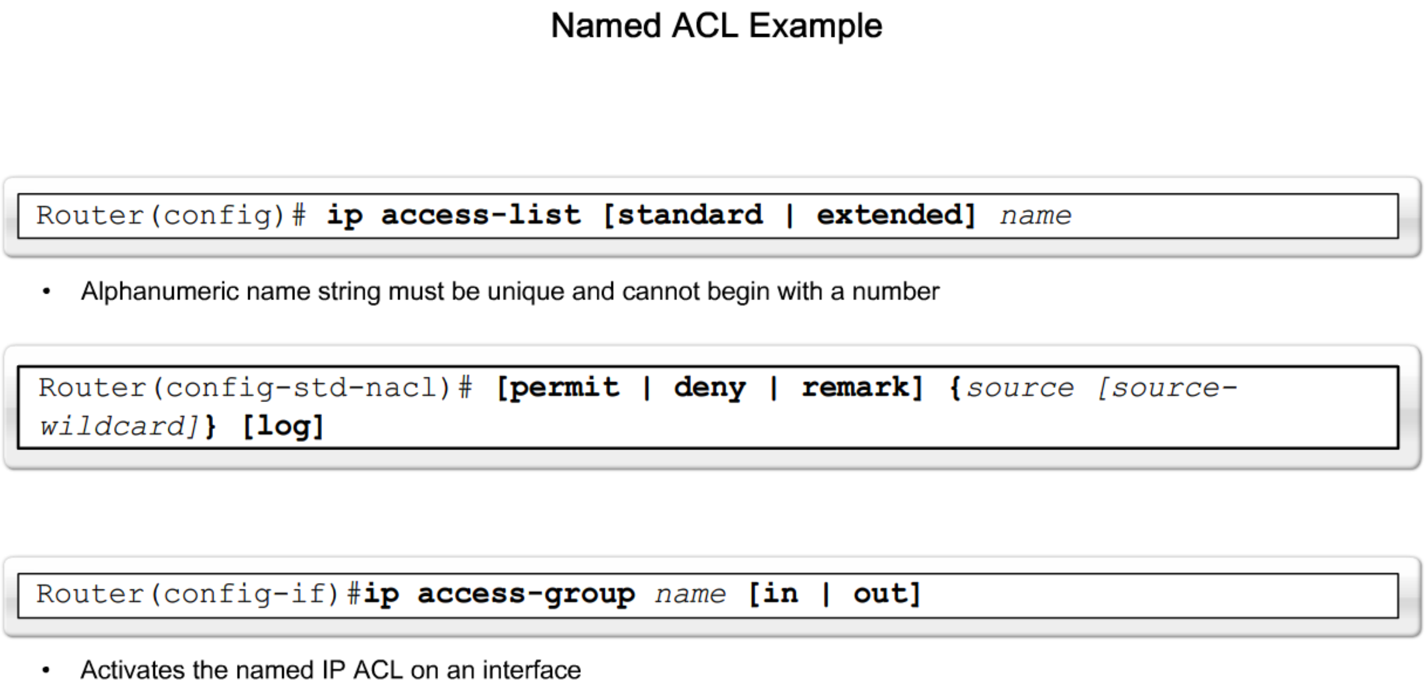
```
access-list 20 permit 192.168.10.11
access-list 20 deny 192.168.10.0 0.0.0.255
```

Step 3

```
R1#conf t
Enter configuration commands, one per line. End with
CTRL/Z.
R1(config)#no access-list 20
R1(config)#access-list 20 permit   192.168.10.100
R1(config)#access-list 20 deny 192.168.10.0 0.0.0.255
```

Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Explain how to create a named ACL



Named ACL Example

```
Router(config)# ip access-list [standard | extended] name
```

- Alphanumeric name string must be unique and cannot begin with a number

```
Router(config-std-nacl)# [permit | deny | remark] {source [source-
wildcard]} [log]
```

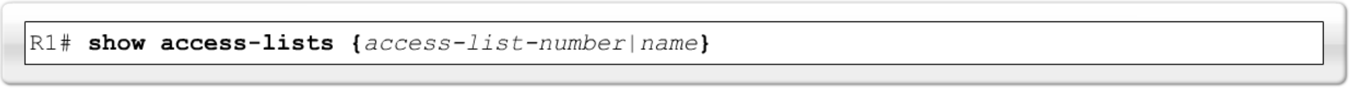
```
Router(config-if)#ip access-group name [in | out]
```

- Activates the named IP ACL on an interface

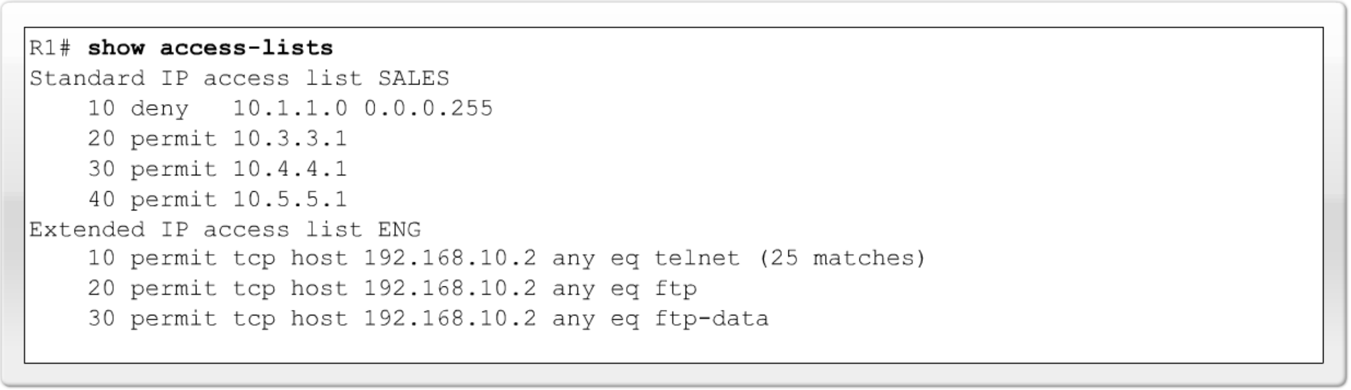
Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Describe how to monitor and verify ACLs

Monitoring ACL Statements



```
R1# show access-lists {access-list-number|name}
```

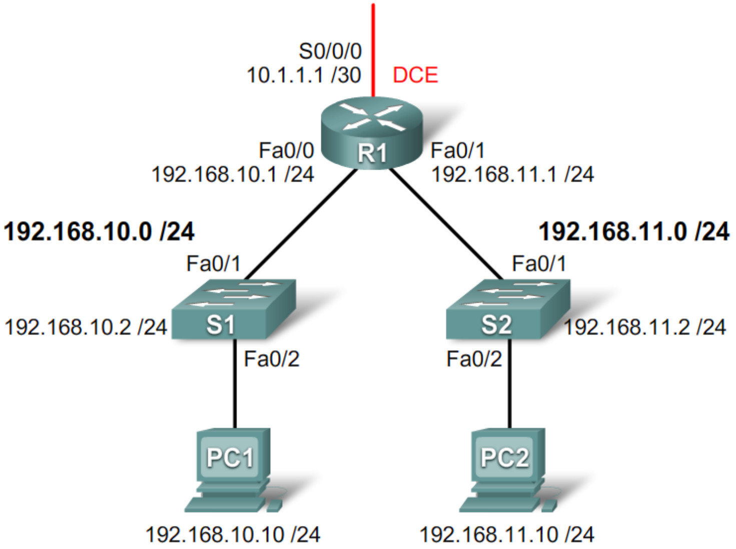


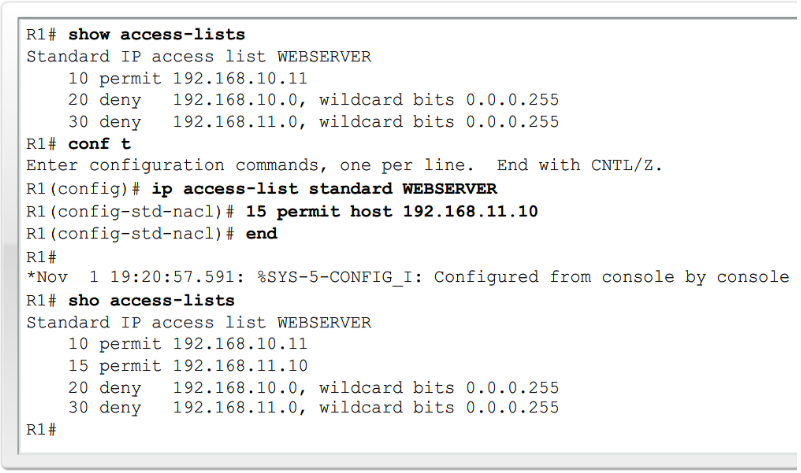
```
R1# show access-lists
Standard IP access list SALES
    10 deny   10.1.1.0 0.0.0.255
    20 permit 10.3.3.1
    30 permit 10.4.4.1
    40 permit 10.5.5.1
Extended IP access list ENG
    10 permit tcp host 192.168.10.2 any eq telnet (25 matches)
    20 permit tcp host 192.168.10.2 any eq ftp
    30 permit tcp host 192.168.10.2 any eq ftp-data
```

Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Explain the process for editing named ACLs

Adding a Line to a Named ACL

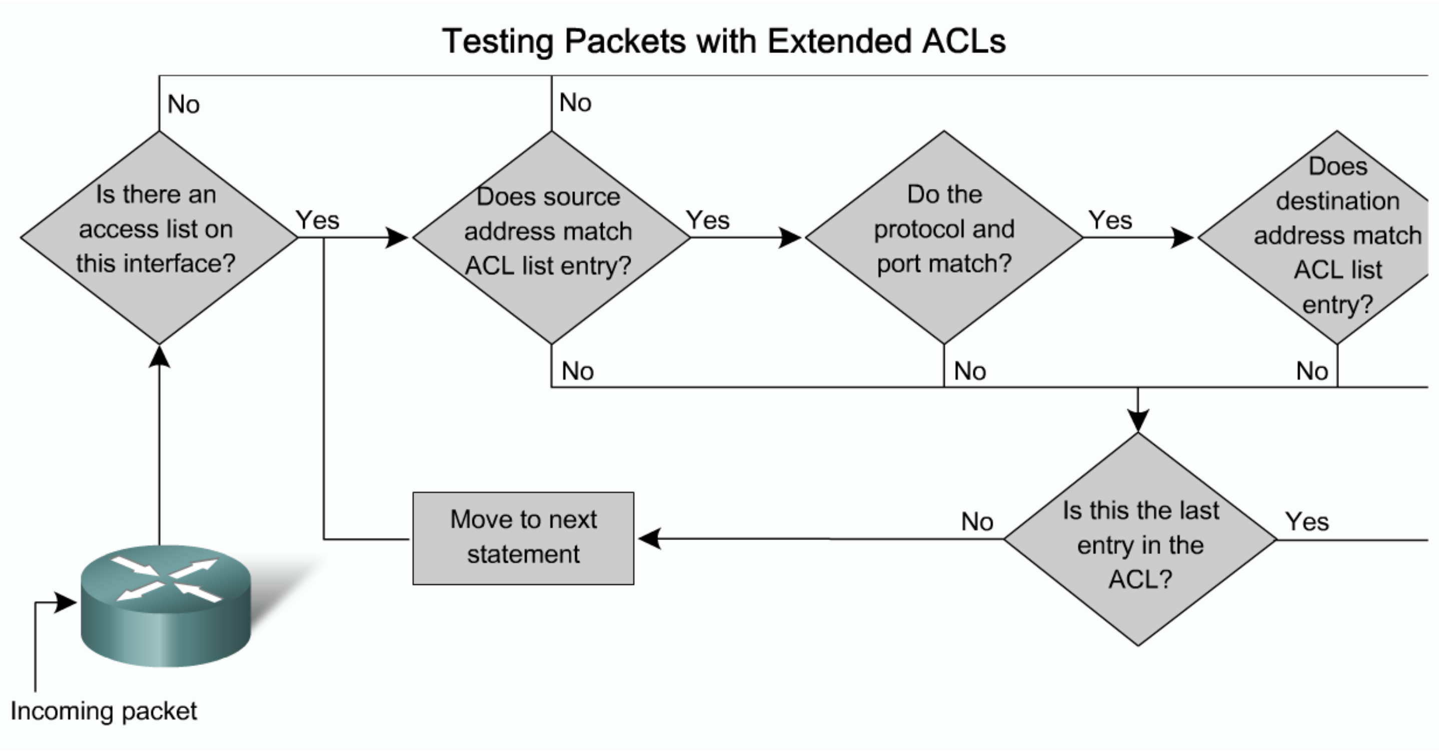




```
R1# show access-lists
Standard IP access list WEBSERVER
    10 permit 192.168.10.11
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list standard WEBSERVER
R1(config-std-nacl)# 15 permit host 192.168.11.10
R1(config-std-nacl)# end
R1#
*Nov  1 19:20:57.591: %SYS-5-CONFIG_I: Configured from console by console
R1# sho access-lists
Standard IP access list WEBSERVER
    10 permit 192.168.10.11
    15 permit 192.168.11.10
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1#
```

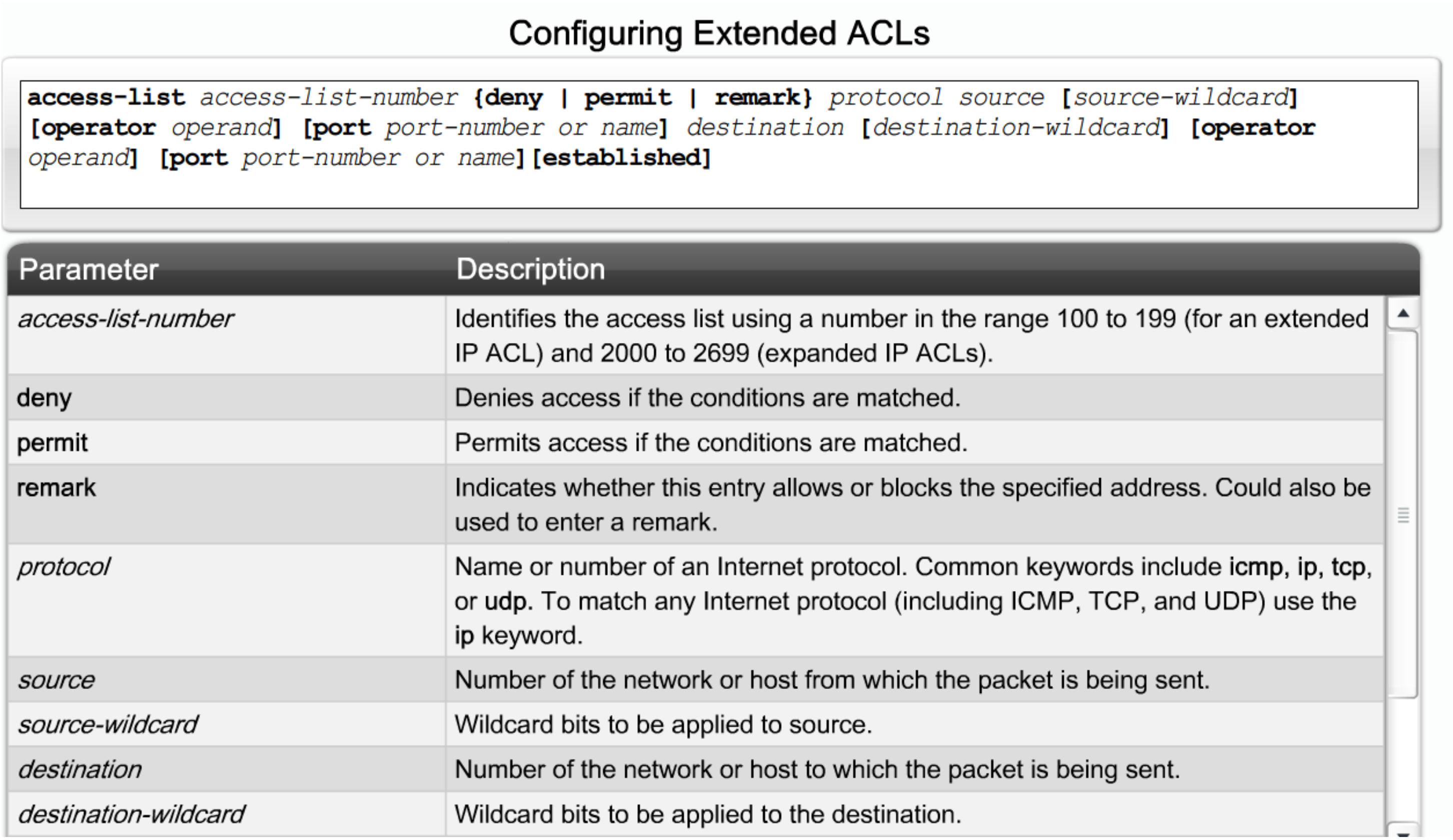
Configure Extended ACLs in a Medium-Size Enterprise Branch Office Network

- Explain how an extended ACL provides more filtering then a standard ACL


Testing Packets with Extended ACLs
No
No
Is there an access list on this interface?
Yes
Does source address match ACL list entry?
Yes
Do the protocol and port match?
Yes
Does destination address match ACL list entry?
No
No
No
Is this the last entry in the ACL?
No
Yes
Move to next statement
Incoming packet

Configure Extended ACLs in a Medium-Size Enterprise Branch Office Network

- Describe how to configure extended ACLs



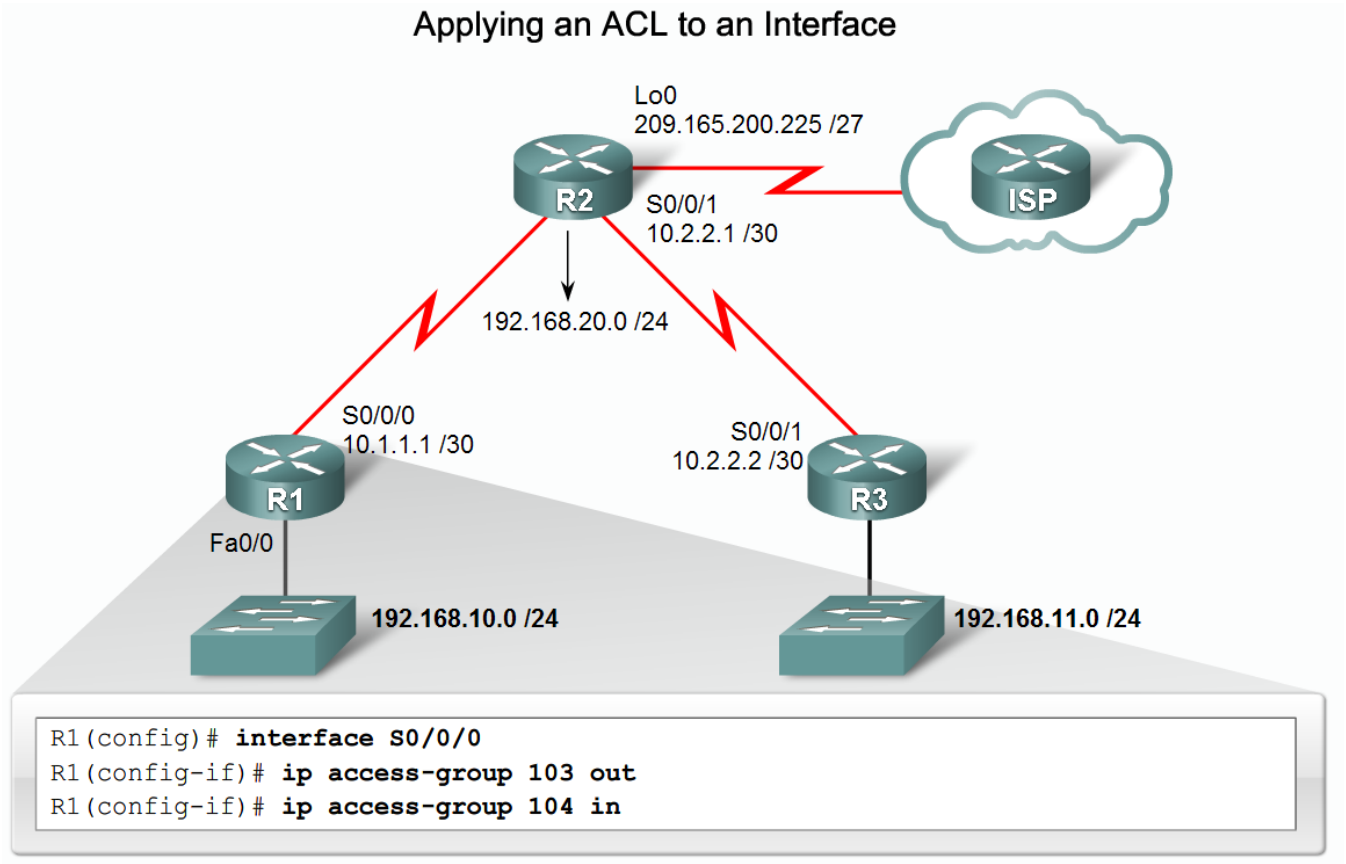
Configuring Extended ACLs

```
access-list access-list-number {deny | permit | remark} protocol source [source-wildcard]
[operator operand] [port port-number or name] destination [destination-wildcard] [operator
operand] [port port-number or name] [established]
```

Parameter	Description
access-list-number	Identifies the access list using a number in the range 100 to 199 (for an extended IP ACL) and 2000 to 2699 (expanded IP ACLs).
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
remark	Indicates whether this entry allows or blocks the specified address. Could also be used to enter a remark.
protocol	Name or number of an Internet protocol. Common keywords include **icmp**, **ip**, **tcp**, or **udp**. To match any Internet protocol (including ICMP, TCP, and UDP) use the **ip** keyword.
source	Number of the network or host from which the packet is being sent.
source-wildcard	Wildcard bits to be applied to source.
destination	Number of the network or host to which the packet is being sent.
destination-wildcard	Wildcard bits to be applied to the destination.

Configure Extended ACLs in a Medium-Size Enterprise Branch Office Network

- Describe how to apply an extended ACL to an interface



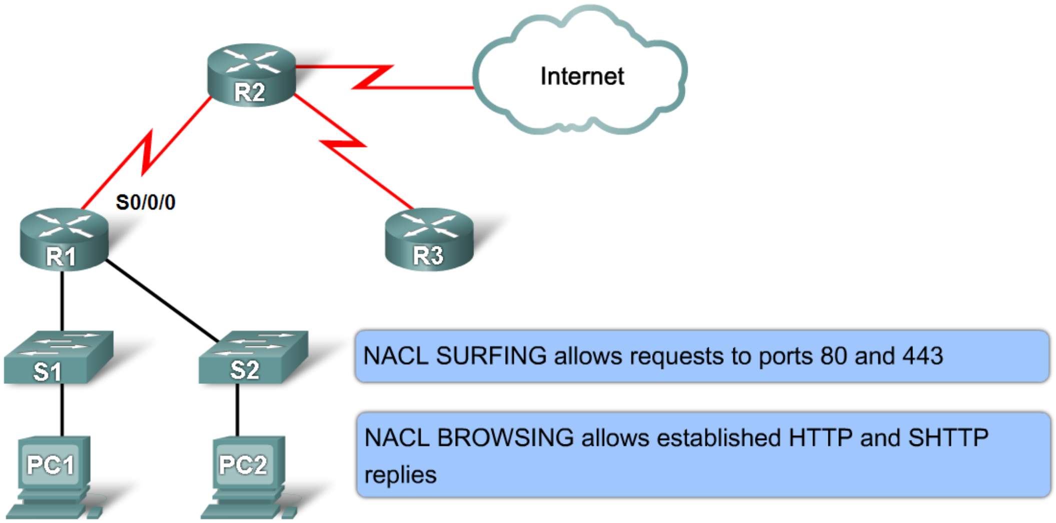
Applying an ACL to an Interface

```
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 103 out
R1(config-if)# ip access-group 104 in
```

Configure Extended ACLs in a Medium-Size Enterprise Branch Office Network

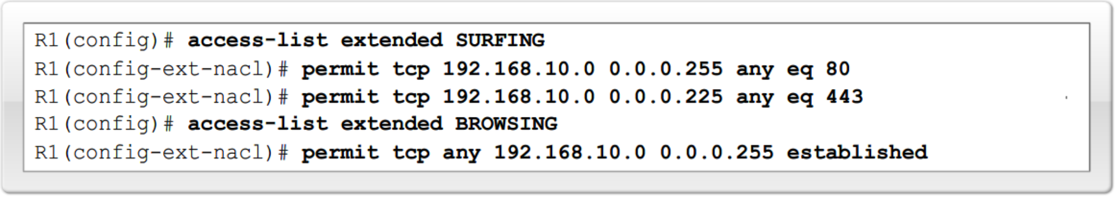
- Describe how to create named extended ACLs

Configuring Named Extended ACLs



NACL SURFING allows requests to ports 80 and 443

NACL BROWSING allows established HTTP and SHTTP replies

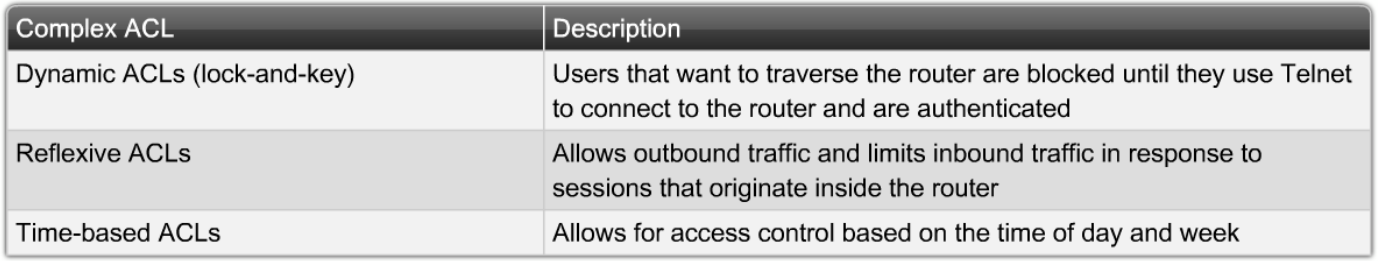


```
R1(config)# access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.225 any eq 443
R1(config)# access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
```

Describe Complex ACLs in a Medium-Size Enterprise Branch Office Network

- List the three types of complex ACLs

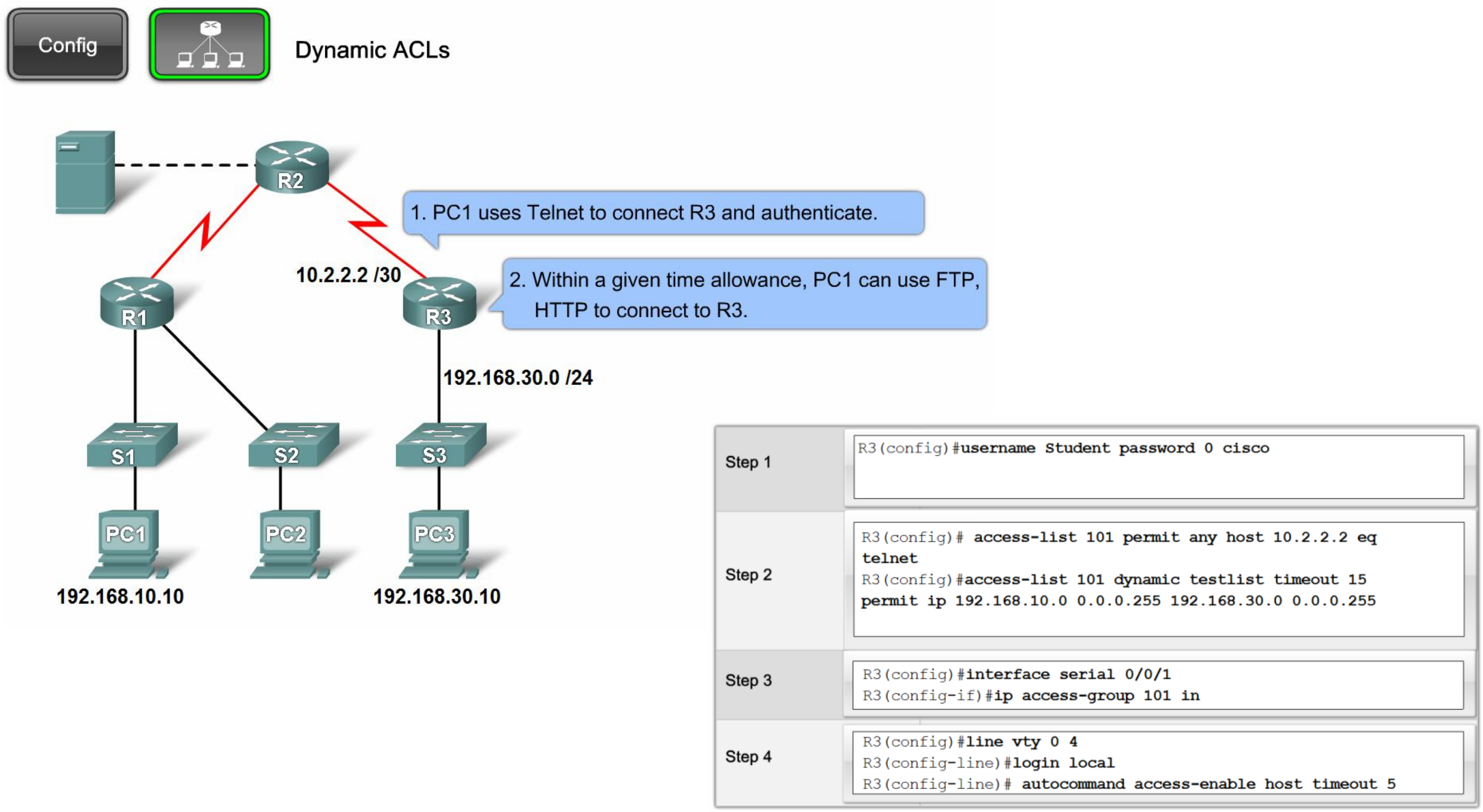
Types of Complex ACLs



Complex ACL	Description
Dynamic ACLs (lock-and-key)	Users that want to traverse the router are blocked until they use Telnet to connect to the router and are authenticated
Reflexive ACLs	Allows outbound traffic and limits inbound traffic in response to sessions that originate inside the router
Time-based ACLs	Allows for access control based on the time of day and week

Describe Complex ACLs in a Medium-Size Enterprise Branch Office Network

- Explain how and when to use dynamic ACLs



1. PC1 uses Telnet to connect R3 and authenticate.

2. Within a given time allowance, PC1 can use FTP, HTTP to connect to R3.

Step 1

```
R3(config)#username Student password 0 cisco
```

Step 2

```
R3(config)# access-list 101 permit any host 10.2.2.2 eq
telnet
R3(config)#access-list 101 dynamic testlist timeout 15
permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

Step 3

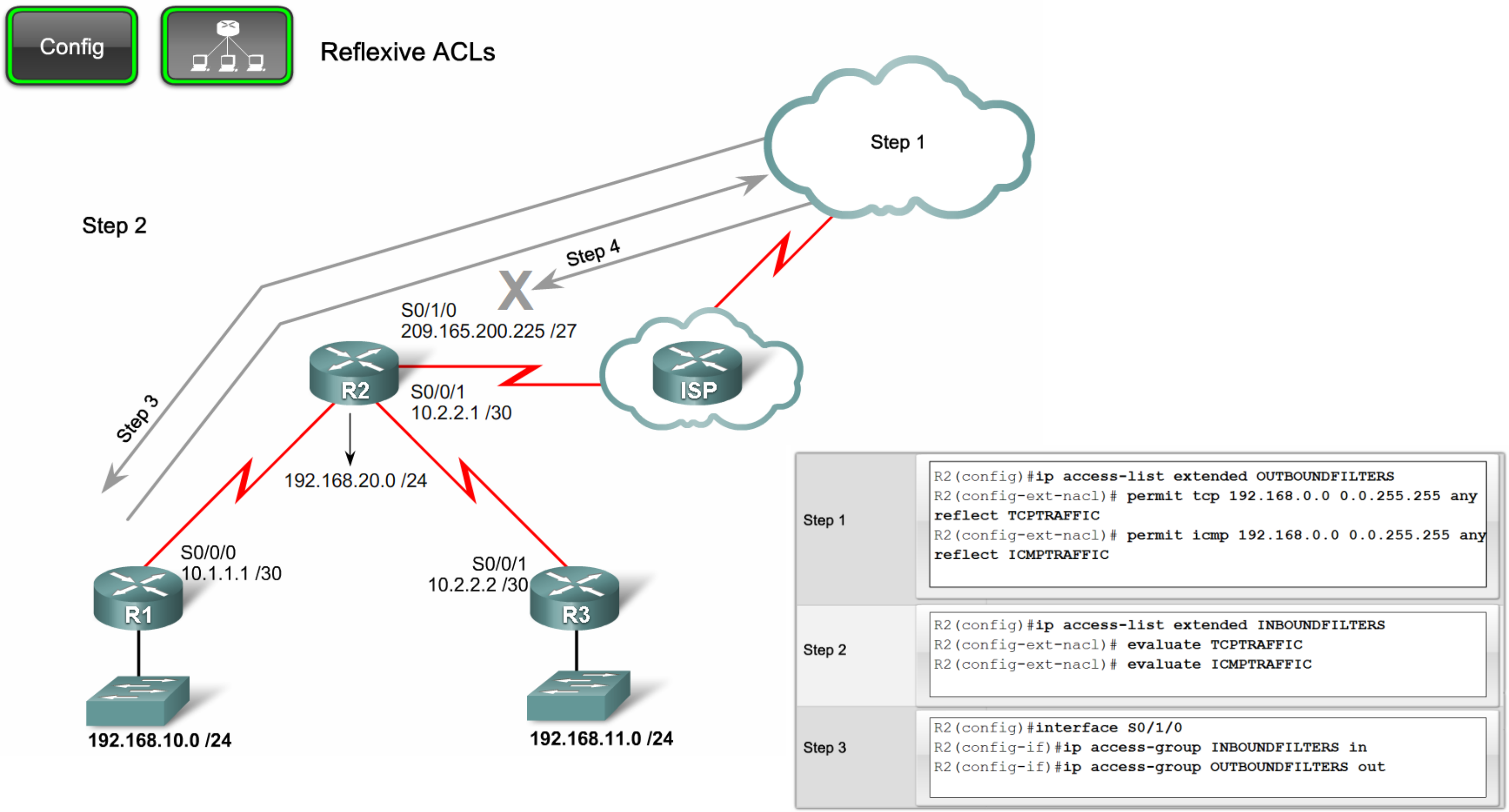
```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group 101 in
```

Step 4

```
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)# autocommand access-enable host timeout 5
```

Describe Complex ACLs in a Medium-Size Enterprise Branch Office Network

- Explain how and when to use reflexive ACLs



Step 1

```
R2(config)#ip access-list extended OUTBOUNDFILTERS
R2(config-ext-nacl)# permit tcp 192.168.0.0 0.0.255.255 any
reflect TCPTRAFFIC
R2(config-ext-nacl)# permit icmp 192.168.0.0 0.0.255.255 any
reflect ICMPTRAFFIC
```

Step 2

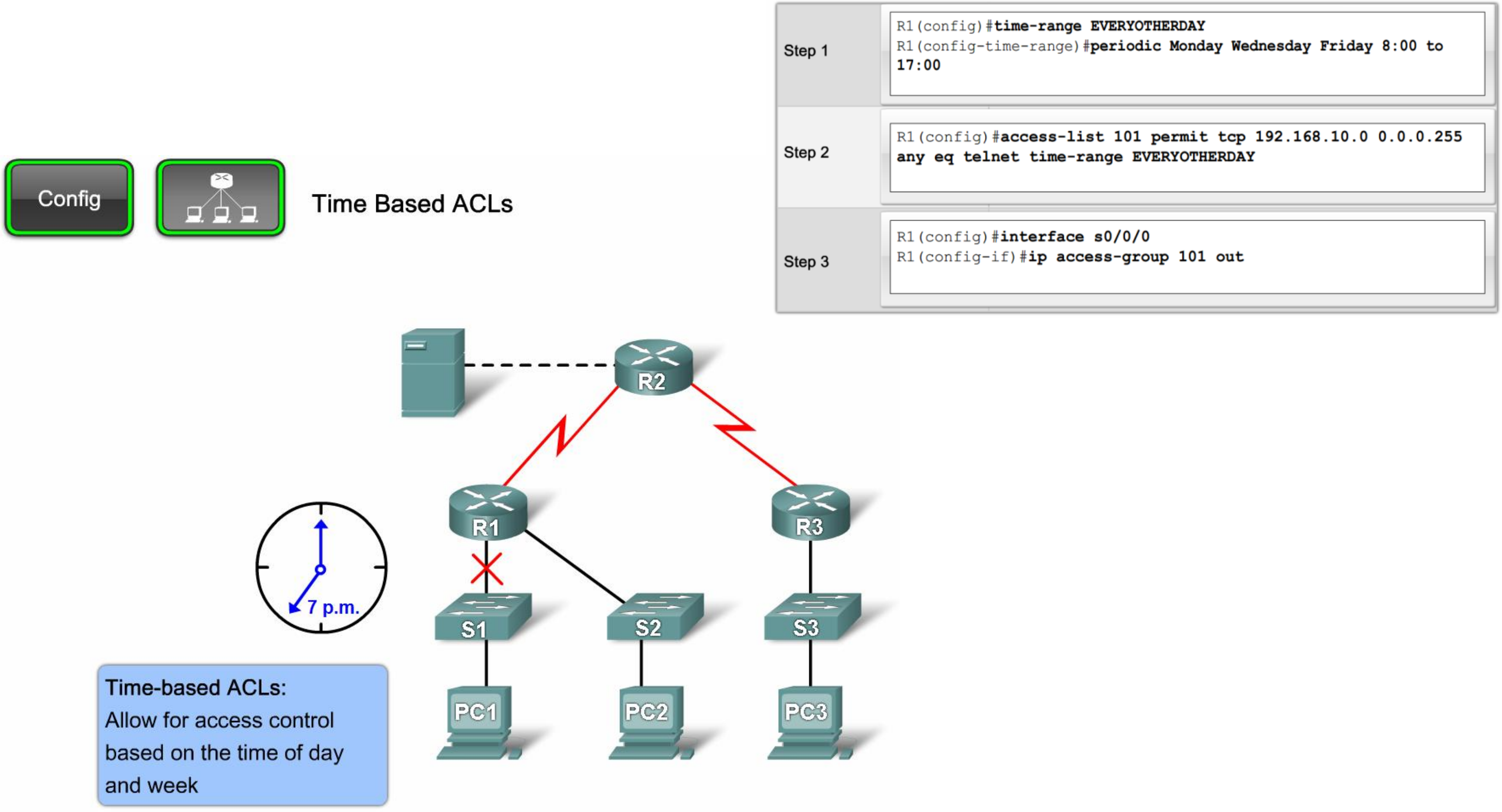
```
R2(config)#ip access-list extended INBOUNDFILTERS
R2(config-ext-nacl)# evaluate TCPTRAFFIC
R2(config-ext-nacl)# evaluate ICMPTRAFFIC
```

Step 3

```
R2(config)#interface S0/1/0
R2(config-if)#ip access-group INBOUNDFILTERS in
R2(config-if)#ip access-group OUTBOUNDFILTERS out
```

Describe Complex ACLs in a Medium-Size Enterprise Branch Office Network

- Explain how and when to use time-based ACLs



Step 1

```
R1(config)#time-range EVERYOTHERDAY
R1(config-time-range)#periodic Monday Wednesday Friday 8:00 to
17:00
```

Step 2

```
R1(config)#access-list 101 permit tcp 192.168.10.0 0.0.0.255
any eq telnet time-range EVERYOTHERDAY
```

Step 3

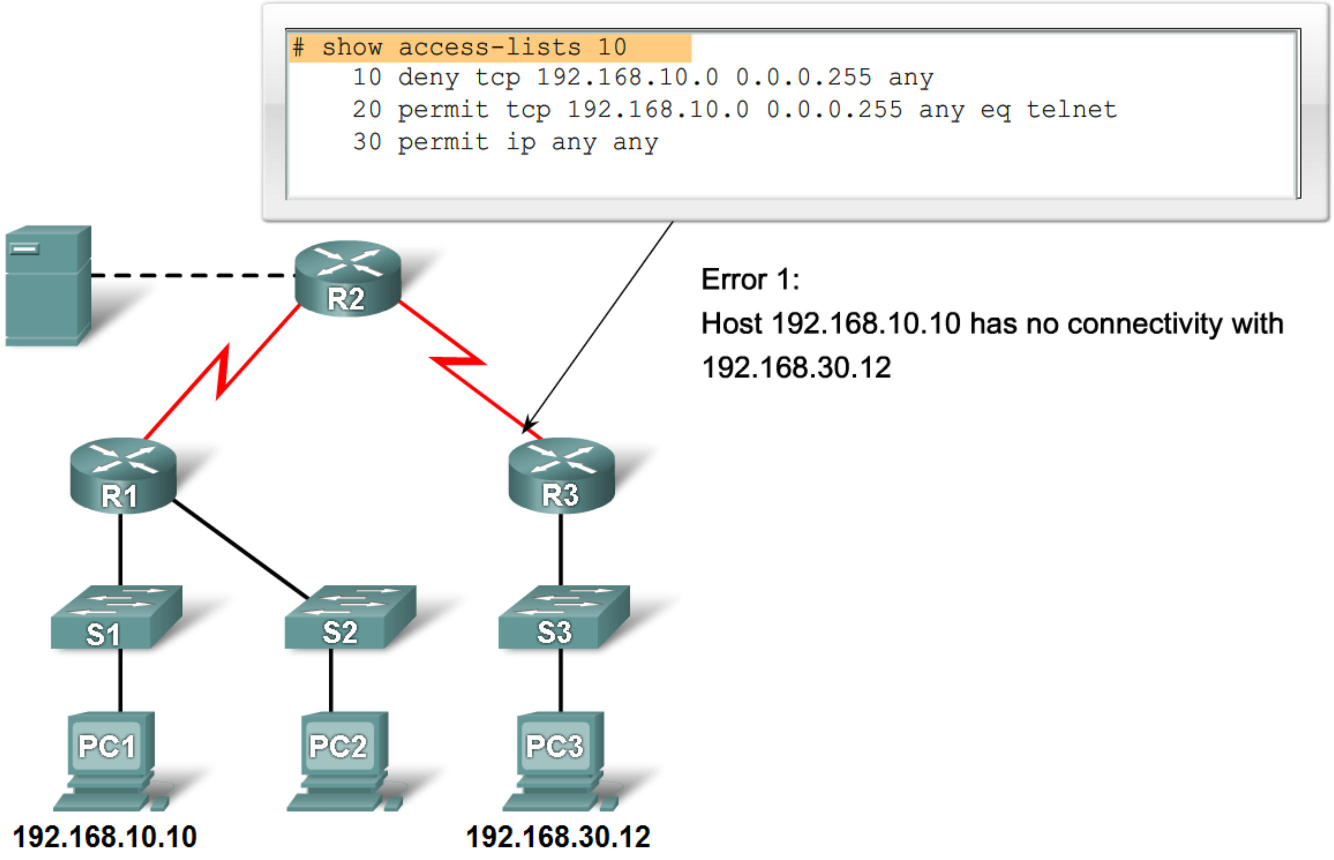
```
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 101 out
```

Time-based ACLs:
Allow for access control based on the time of day and week

Describe Complex ACLs in a Medium-Size Enterprise Branch Office Network

- Describe how to troubleshoot common ACL problems

Troubleshooting Common ACL Errors



```
# show access-lists 10
    10 deny tcp 192.168.10.0 0.0.0.255 any
    20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
    30 permit ip any any
```

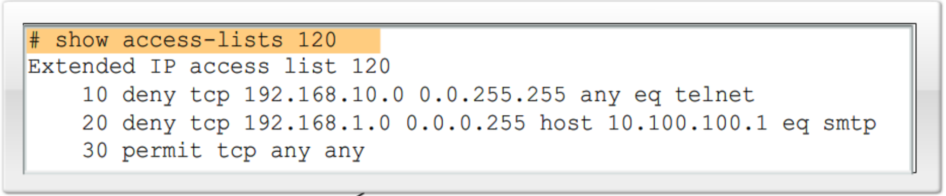
Error 1:

Host 192.168.10.10 has no connectivity with 192.168.30.12

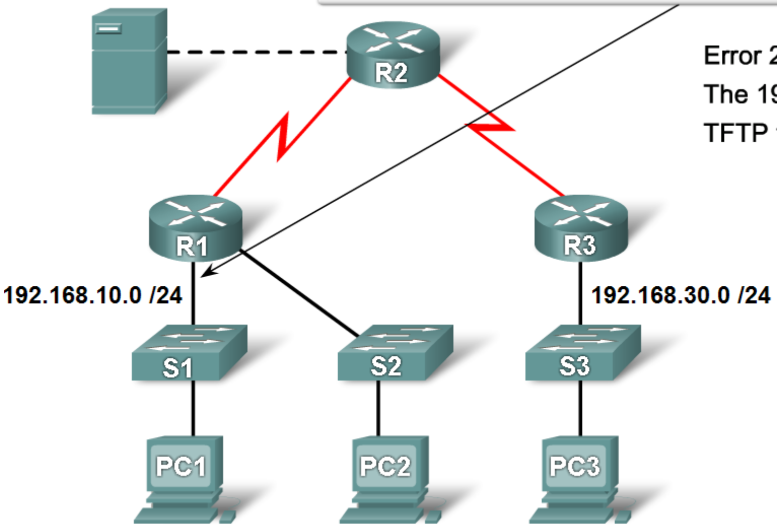
Implement, Verify and Troubleshoot ACLs in an Enterprise Network Environment

- Create, place and verify a standard/ extended ACL and verify its placement.
- Verify ACL’s functionality and troubleshoot as needed.

Troubleshooting Common ACL Errors



```
# show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.255.255 any eq telnet
    20 deny tcp 192.168.1.0 0.0.0.255 host 10.100.100.1 eq smtp
    30 permit tcp any any
```



Error 2:
The 192.168.10.0 /24 network cannot use TFTP to connect to the 192.168.30.0 /24.

Summary

- An Access List (ACL) is:

  A series of permit and deny statements that are used to filter traffic

- Standard ACL
  - –Identified by numbers 1 - 99 and 1300 - 1999
  - –Filter traffic based on source IP address
- Extended ACL
  - –Identified by number 100 -199 & 2000 - 2699
  - –Filter traffic based on
    - •Source IP address
    - •Destination IP address
    - •Protocol
    - •Port number

Summary

- Named ACL
  - –Used with IOS 11.2 and above
  - –Can be used for either standard or extended ACL
- ACL’s use Wildcard Masks (WCM)
  - –Described as the inverse of a subnet mask
    - •Reason
      - –0 → check the bit
      - –1 → ignore the bit

Summary

- Implementing ACLs
  - –1st create the ACL
  - –2nd place the ACL on an interface
    - •Standard ACL are placed nearest the destination
    - •Extended ACL are placed nearest the source
- Use the following commands for verifying & troubleshooting an ACL
  - –Show access-list
  - –Show interfaces
  - –Show run

Summary

- Complex ACL
    - –Dynamic ACL
    - –Reflexive ACL
    - –Time based ACL